
# FinTech and the Existing Legal Framework for Anti-Money Laundering and Counter-Terrorism Financing*†

Jim Sivon

June, 2015

On May 5, 2015, the Financial Crimes Enforcement Network ("FinCEN") imposed a $700,000 civil fine against Ripple Labs, Inc. ("Ripple Labs") for violations of federal anti-money laundering ("AML") requirements.[1] Ripple Labs operates an open-source system for clearing and settling payments, including a math-based currency called XRP. The fine was based upon Ripple Lab's failure to register as a money service business, to implement an anti-money laundering program, and to report suspicious activities related to several financial transactions.

The fine imposed upon Ripple Labs signals that companies at the intersection of technology and finance ("FinTech") must pay attention to compliance with existing anti-money laundering and counter-terrorism financing requirements. This case also suggests that it may be time to re-examine the existing legal framework for addressing money laundering and terrorism financing, and that technologies employed by FinTech companies may be useful in designing alternative approaches to detecting and preventing money laundering and terrorist financing.

The existing legal framework for addressing money laundering and terrorism financing is rooted in reporting and record keeping requirements imposed by the Bank Secrecy Act ("BSA") in 1970.[2] In the past 45 years, however, advances in technology have transformed financial transactions. In 1970, the Internet did not exist; Microsoft and Apple had yet to be founded; and bank ATM's had just been introduced. Today, companies such as Ripple Labs are engaged in activities that were not envisioned by the authors of the Bank Secrecy Act.



†The information contained in this newsletter does not constitute legal advice. This newsletter is intended for educational and informational purposes only.

[1] *In the Matter of Ripple Labs Inc. and XRP II, LLC*, Financial Crimes Enforcement Network, Order Number 2015-05.

[2] P.L. 91-508; 12 U.S.C.A. §1829b; 12 U.S.C.A. §§1951-1959; 18 U.S.C.A. §1956, §1957 and §1960; 31 U.S.C.A. §§5311-5314; and 31 U.S.C.A. §§5316-5332.

***A Short History of the Bank Secrecy Act***

The Bank Secrecy Act was passed in response to concerns over the use of secret foreign banking accounts to facilitate illegal activities and a lack of recordkeeping by banks to assist law enforcement agencies. The Act established recordkeeping and reporting requirements for financial institutions, including the submission of Currency Transaction Reports ("CTRs") to the federal government. It also established civil and criminal penalties for failure to comply with record keeping and reporting requirements.

The Bank Secrecy Act has been amended on several occasions since 1970. In 1986, Congress amended the Act to address "structuring" transactions that were designed to evade the Act's reporting and recordkeeping requirements.[3] The 1986 amendments also made money laundering a federal crime and directed the federal banking agencies to require financial institutions to establish and implement anti-money laundering policies and procedures. In 1992, the Annunzio-Wylie Anti-Money Laundering Act amended the Bank Secrecy Act to impose an obligation on banks to file Suspicious Activity Reports ("SARs") and to report wire transfers.[4] The 1992 amendments also gave regulators the authority to revoke a bank's charter for the conviction of a money laundering offense. In 1994, the Money Laundering Suppression Act amended to the Bank Secrecy Act to address the growing burdens associated with the CTR filing requirement.[5] The 1994 amendments created a framework for financial institutions to exempt certain customers from CTR filings. Those amendments extended the requirements of the Bank Secrecy Act to Money Service Businesses ("MSBs"). Finally, in 2001, as part of the USA Patriot Act, Congress extended the basic reporting and recordkeeping framework of the Bank Secrecy Act to the financing of terrorism.[6]

In summary, the legal framework established in the Bank Secrecy Act has evolved and been expanded over time, but the basic framework of the Act — recording and reporting financial transactions to federal authorities — has remained unchanged since 1970.

***The Efficacy of the Existing Legal Framework***

According to FinCEN, the reporting requirements imposed by the Bank Secrecy Act result in over 50,000 filings everyday by banks and other covered financial firms.[7] This data includes SARs, CTRs, and other reports and is used by over 10,000 agents, analysts, and investigators at over 350 separate agencies.[8]

Unquestionably this data is important in individual law enforcement cases. Yet, in the forty years since the passage of the Bank Secrecy Act, it is not apparent that this recordkeeping and reporting regime has been effective at curbing money laundering or terrorist financing. A report by the United Nations' Office on Drugs and Crime estimates that in 2009 criminals may have laundered approximately $2.6 trillion, or 2.7% of global GDP.Regulators and law enforcement authorities also continue to cite financial firms for violations of the recording keeping and reporting requirements.[9]

[3]Money Laundering Control Act of 1986, P.L. 99-570.
[4]Title XV of P.L. 102-55.
[5]Title IV of P.L. 103-325.
[6]P.L. 107-56.
[7]Statement of Jennifer Shasky Calvery, Director, Financial Crimes Enforcement Network before the Institute of International Bankers Annual Anti-Money Laundering Seminar, April 30, 2015.
[8]Id.
[9]Recent examples include a $20 million civil fine to Oppenheimer & Co (January 2015); a $2.05 billion fine to JPMorgan

The persistence of money laundering and terrorist financing raises questions about the efficacy of the current recording keeping and reporting requirements of the Bank Secrecy Act. The current Director of FinCEN has sought to dispel these questions: "please know that your information is neither going into a black hole, nor being stove piped in just one or a few agencies as has often been the perception. The reality is quite the opposite."[10] However, data demonstrating the linkage between current reporting requirements and law enforcement investigation is limited. On its web site, FinCEN lists examples in which SAR data has been instrumental in law enforcement investigations, but does not publish a comprehensive list of such cases.[11] Furthermore, data published by the Internal Revenue Service ("IRS") shows a sizable gap between SAR filings and investigations. In 2013, there were over 1.6 million SARs filed,[12] but IRS reports only 922 investigations initiated based upon SAR filings that year.[13] Thus, the limited data that is available on the value of current reporting requirements perpetuates questions about the efficacy of the current reporting requirements.

***Unintended Consequences of the Existing Legal Framework***

The current system also has generated some unintended consequences. One such consequence is so-called "defensive" filings of SARs.[14] Some financial institutions file SARs for defensive purposes in order to minimize the potential sanctions associated with a failure to file. Another unintended consequence of the current system is the "de-risking" of customers.[15] This is a practice in which a financial institution firms voluntarily will cease to do business with certain categories of customers in order to minimize the potential for a BSA-related violation.

It may be argued that both of these practices are contrary to the public interest. Defensive filings impose a needless burden on law enforcement authorities, which end up reviewing files that may have little relationship to money laundering or terrorism financing. De-risking makes it difficult for certain categories of firms to obtain needed financial services.

***A Recent Interagency Review of Existing Legal Framework***

Treasury and other federal financial regulators recently conducted a review of the existing legal framework for addressing money laundering and terrorism financing.[16] Based upon that review, the agencies recommended actions to address perceived gaps in the current system. The agencies called for clarifying the safe harbor for filing SARS, clarifying the ability of firms to share AML and counter-terrorist financing ("CTF") information, and applying AML and CTF recordkeeping requirements to more categories of firms. These are

Chase for failing to file SARs in connection with the Madoff scheme (January 2014); a $90 million fine to TD Bank for failing to file SARs relating to South Florida-based Ponzi scheme (September 2013); a $1.9 billion fine to HSBC (December 2012); and a $100 million forfeiture to MoneyGram related to mass marketing and consumer fraud phishing schemes and failure to maintain adequate AML program (November 2012).

[10] Statement of Jennifer Shasky Calvery, Director, Financial Crimes Enforcement Network before the Institute of International Bankers Annual Anti-Money Laundering Seminar, April 30, 2015.

[11] ***Investigations Assisted by FinCEN Data***

[12] SAR Stats Techical Bulletin, Financial Crimes Enforcement Network, July 2014.

[13] ***Statistical Data - Money Laundering & Bank Secrecy Act (BSA)***

[14] *Suspicious Activity Report Use Is Increasing, but FinCEN Needs to Further Develop and Document Its Form Revision Process*, General Accountability Office, GAO-09-226, Feb. 2009.

[15] See "Dirty-Money Crackdown Pinches Bank Customers", Wall Street Journal, May 26, 2015, p. A.1.

[16] ***Remarks of Treasury Under Secretary Cohen at the ABA/ABA Money Laundering Enforcement Conference, Nov. 10, 2014.***

reasonable changes to the current system. It would appear, however, that the agencies missed an opportunity to take a broader view of the system and reassess the framework within the context of a changing industry and evolving technologies.

***FinTech and Alternative Approaches to the Existing Legal Framework***

One federal banking regulator, the Comptroller of the Currency, has acknowledged that the current legal framework for addressing money laundering and counter-terrorist financing should be updated to remain effective: "The current regulatory regime, which is rooted in 20th century concepts and approaches, will need to change and adopt in order remain relevant into the 21st century."[17] FinTech companies are a 21st century development, and the technological innovations that are propelling those firms, including data mining and artificial intelligence systems, could be a key to the creation of alternative approaches to detecting and preventing money laundering and terrorist financing.

*Jim Sivon is a partner with the law firm of* ***Barnett Sivon & Natter, P.C.***

[17] Remarks by Thomas J. Curry Comptroller of the Currency Before the Institute of International Bankers Washington, D.C. March 2, 2015.